모바일 콘텐츠 유통에 적합한 ID 기반 디지털 서명 기법

윤성현
백석대학교 정보통신학부

The Mobile ID based Digital Signature Scheme Suitable for Mobile Contents Distribution

Sung-Hyun Yun
Division of Information & Communication Engineering, Baekseok University

요 약 스마트폰의 보급으로 모바일 상거래가 급속하게 성장함에 따라서 모바일 콘텐츠에 대한 저작권 보호 및 분배 문제가 주요 이슈로 떠오르고 있다. 스마트폰은 장소에 관계없이 항상 소지할 수 있어서 활용성이 매우 높으며 USIM(Universal Subscriber Identity Module)을 등록하여 사용하기 때문에 사용자 ID를 대표하는 수단으로 사용될 수 있다. 본 논문에서는 모바일 ID 기반의 디지털 서명 기법을 제안한다. 모바일 ID는 스마트폰의 USIM 정보와 사용자가 임의로 생성한 난수 값을 이용하여 생성한다. 더불어 제안한 서명 기법의 도전-응답 방식의 검증 프로토콜은 스마트폰에서 ID 기반의 모바일 투표, 모바일 콘텐츠 분배 등의 응용에 적용될 수 있다.

• **주제어** : 이동보안, 이동신분증, 신분증기반 서명, 명백한 서명, 콘텐츠 분산

Abstract The wide use of mobile devices such as smart phones makes the mobile commerce industry be growing-up rapidly. In mobile commerce security, how to secure a copyright of mobile contents and how to distribute it are of major concerns. The user can carry the smart phone regardless of the places. Thus the utilization of it is very high than that of personal computers. The USIM(Universal Subscriber Information Module) inserted in the smart phone binds the user with the device. This means that the smart phone can be used to represent the owner's identity. In this paper, we develop the mobile ID based digital signature scheme. We create the mobile ID by combining USIM with the user's random secret value. In addition, undeniable property of our signature scheme can make ID based applications such as mobile voting and mobile content distribution be possible with the smart phone.

• **Key Words** : Mobile Security, Mobile ID, ID based Signature, Undeniable Signature, Contents Distribution

1. 서론

모바일 상거래는 스마트폰과 같은 무선 망 이용이 가능한 휴대기기를 이용하여 상품을 거래하는 것을 의미한다. 스마트폰은 그 특성상 항상 휴대할 수 있기 때문에 활용성이 매우 높고 이에 기반을 둔 모바일 상거래가 사용 장소에 제한을 받는 PC 기반의 전자상거래보다 급속히 성장할 것으로 예상된다. 상거래 모델은 상품의 유형에 따라서 달라지는데 본 논문에서는 모바일 기기에서 재생이 가능한 음악, 오디오, 비디오, 게임, 앱 등과 같은 디지털 콘텐츠를 온라인으로 거래하는 모델을 대상으로 한다.

사용자 인증은 제 3자에게 자신을 입증하는 방법으로 내가 기억하고 있는 것 또는 내가 가지고 있는 것을 이용

*교신저자 : 윤성현(shyoon@bu.ac.kr)
접수일 2011년 1월 5일 수정일 2011년 3월 25일 게재확정일 2011년 3월 27일

하여 증명한다. 일반적으로 가장 많이 사용되는 아이디/패스워드 기반의 사용자 인증은 내가 기억하고 있는 것에 기반을 둔다. 인증을 위해서 별도의 카드 및 이를 확인할 장비가 필요 없기 때문에 사용 편의성이 높고 보급률이 높다.

단점은 아이디/패스워드가 노출되었을 경우에 제 3자에 의한 가장 및 위장 공격이 가능하다는 것이다. 사람들이 많이 사용하는 네이트 온, 트위터, 페이스 북 등과 같은 소셜네트워크 서비스를 통하여 제 3자가 나 임을 가장하여 피해를 줄 수 있다. 인터넷은 대면 공간이 아니기 때문에 로그인한 대화 상대방에 대해서 확인할 수 없다. 아이디/패스워드 정보를 상대방 만 알고 있다는 가정 하에서 가상의 공간에서 사용자 인증이 이루어지고 있다.

주민등록증, 스마트 ID 카드를 이용하는 것은 내가 가지고 있는 것으로 사용자 인증을 수행하는 방법이다. 기억하고 있는 것에 기반을 둔 방법에 비해서 정보의 노출 위험성이 적고 특히 주민등록증 및 ID 카드는 본인과 카드를 결합하기 때문에 제 3자에 의한 가장 공격이 아이디/패스워드 방식보다 어렵다. 아이디/패스워드 방식은 개인의 기억에 의존하기 때문에 소유자와의 물리적 결합이 없다.

주민등록증은 모든 사람이 소지하고 있지만 전자식 카드가 아니므로 컴퓨터, 인터넷 상의 서버에 인증 수단으로 사용할 수 없다. ID 카드는 특정 목적을 위해서 만들어진 스마트카드로 사용자 수가 제한적이다. 스마트카드는 범용의 목적으로 사용될 수 있지만 발행 회사도 다르고 사용되는 운영체제도 다르고 목적에 따라서(용도에 따라서) 다른 형태로 발급되는 것이 일반적이다. 범용화된 사용자 인증 인터페이스로 사용될 수 없다. 스마트카드처럼 프로그램이 가능하며 주민등록증처럼 범용으로 사용이 가능한 인증 수단은 무엇인가 ?

휴대폰은 USIM을 개인별로 등록해야만 사용이 가능하다. 발급은 오프라인에서 본인 확인 후 이루어지며 공인 인증서 발급 절차와 유사하다. 컴퓨터와 인터넷을 이용한 가상의 공간에서 법적 구속력이 있는 ID(키)를 만들기 위해서는 반드시 신뢰할 수 있는 제 3자(또는 기관)의 승인 절차가 포함되어야 한다. 온라인은 익명의 공간이기 때문에 해당 절차에 오프라인에서의 신분확인이 반드시 포함되어야 한다.

스마트폰은 컴퓨터 기능과 전화기 기능이 융합된 장비로 [2] 사용자 인증 과정을 거쳐서 USIM 등록을 해야만 사용할 수 있다. 따라서 주민등록증과 같이 사용자를 대표하는 인증 수단으로 활용될 수 있으며 ID 기반의 보안 프로토콜 [6,7]을 실용화할 수 있는 최적의 플랫폼이다.

온라인은 익명의 공간이기 때문에 주민번호 노출 및 도용으로 인한 개인 프라이버시 침해 문제가 빈번하게 발생한다. 이 경우에 주민등록번호를 취소하고 다시 재발급 받을 수 없기 때문에 많은 사회적 문제를 야기한다. 스마트폰 USIM 정보를 그대로 ID로 사용할 경우에 재발급을 받기 위해서는 다시 등록 과정을 거쳐야하기 때문에 사용자에게 불편을 초래한다. 따라서 ID 도용 시 온라인으로 재발급 받을 수 있는 방법이 필요하다.

본 논문에서는 스마트폰을 활용한 ID 기반의 부인봉쇄 서명 기법을 제안하고 이를 활용한 모바일 콘텐츠 분배 방안에 대해서 논의한다. 스마트폰은 PC와 같이 범용 프로그램을 수행할 수 있는 컴퓨터이기 때문에 모바일 상거래를 가능하게 하는 핵심 구성요소이다. 특히, USIM은 신용카드, 주민등록증과 같이 사용자와 스마트폰을 연결해주기 때문에 PC에서 구현하기 어려웠던 ID 기반의 정보보호 기법의 실용화를 가능하게 해준다.

모바일 디지털 콘텐츠는 사용자 휴대기기에 저장 및 재생할 수 있는 음악, 동영상, 게임 형태의 디지털 데이터로 원본과 복사본의 내용이 동일하고 조작 및 복제 시 이를 구분할 수 없다. 따라서 상거래 데이터로 사용하기 위해서는 디지털 서명과 같이 법적 구속력을 부여할 수 있는 인증 기법의 적용이 필수적이다.

콘텐츠 보안과 관련된 기존의 연구[5]는 대부분 워터마킹, 핑거프린팅 등 저작권 보호를 위한 기법에 초점을 맞추고 있다. 콘텐츠 판매와 관련하여 저작자의 권익을 보장하는 연구는 미흡하다. 저작자는 자신이 만든 콘텐츠로 비즈니스를 할 때 정당한 수익을 기대할 수 있어야 한다. 저작자의 권익을 보장할 수 있는 콘텐츠 분배 프로토콜에 대한 연구가 필요하다.

일반적으로 디지털 콘텐츠는 저작권, 제어 정보, 서명 등을 포함한 패키지 형태로 유통된다. 저작자의 위임을 받은 판매자와 구매자 간에 콘텐츠 거래가 이루어지며 거래 후에 콘텐츠를 활성화하기 위하여 라이센스 및 서명 검증을 한다. 패키지에 서명된 저작자의 일반 서명은 자체검증 기능을 갖기 때문에 저작자가 직접 콘텐츠 검증에 참여할 수 없다. 이 경우 저작자는 거래를 위임한 판매자의 신뢰성에 전적으로 의존할 수 밖에 없다.

판매 및 콘텐츠 인증 과정을 분리하여 패키지 인증 시 저작자가 직접 개입하도록 하면 콘텐츠 유통이 투명해지고 권익을 보장받을 수 있다. 부인봉쇄 서명 기법에서 서

명자는 서명 검증을 요구하는 사용자를 직접 지정할 수 있다.

2 장에서는 재발급이 가능한 모바일 ID 및 디지털 키 생성 방법에 대해서 제안한다. 3 장에서는 모바일 ID 기반의 부인봉쇄 서명 기법을 제안하고 4 장에서 제안한 기법의 부인봉쇄 특성을 분석한다. 5 장에서는 모바일 콘텐츠 거래 시 저작권자의 권익을 보장할 수 있는 콘텐츠 분배 방안에 대해서 논의한다.

2. 모바일 ID를 이용한 디지털 키 생성

모바일 ID 생성 및 이에 기반을 둔 키 생성 기법에 대해서 설명한다. 모바일 ID는 스마트폰 USIM과 패스코드를 이용하여 생성한다. 패스코드는 사용자가 임의로 생성한 난수 값으로 모바일 ID가 도용되었을 경우에 모바일 ID를 재등록할 수 있도록 한다. USIM을 재등록하지 않고 사용자 패스코드만 변경함으로써 다양한 형태의 모바일 ID를 만들어 낼 수 있다.

2.1 모바일 ID 관리 기반

인증받은 USIM을 이용하여 모바일 ID를 생성하면 ID 재발급 시 USIM 등록을 다시 해야 한다. 따라서 효율적인 ID 관리를 위해서 모바일 ID를 온라인으로 등록 및 관리하는 기반이 필요하다. 모바일 ID 관리 기반은 모바일 센터, 디렉토리, MRL (Mobile ID Revocation List)로 구성된다.

모바일 센터는 사용자 ID에 대한 서명, 보관, 조회 등의 업무를 수행하고 인증된 ID를 디렉토리에 등록한다.

디렉토리는 네트워크 DB로 인증된 ID와 취소된 ID를 등록하고 각각의 ID에 권한을 부여하여 모바일 센터를 제외한 일반 사용자들은 다른 사용자의 ID를 조회할 수 없도록 한다.

MRL은 ID 도용으로 인하여 사용자가 기존의 ID를 취소하고 새로운 모바일 ID를 생성한 경우에 기존의 ID를 이용할 수 없도록 따로 보관하고 관리하는 역할을 한다. 모바일 ID와 연동된 웹사이트 로그인 시 취소된 ID로 로그인할 수 없도록 모니터링 한다.

2.2 모바일 ID 및 디지털 키 생성

[정의 1] GF(p)는 암호학적으로 안전한 유한체이고 g는 GF(p) 상에서 정의된 생성자로 위수 p-1을 갖는다[3]. 모바일 ID 인증센터의 공개키 및 개인키는 다음과 같다고 가정한다.

$$sk_{MC} \in Z_{p-1} \ , \ pk_{MC} \equiv g^{sk_{MC}} (\mathrm{mod} p)$$

스마트폰 사용자는 다음과 같이 모바일 ID를 등록 한다.

단계 1: 사용자는 오프라인으로 신분확인을 하고 스마트폰 USIM을 기기에 등록한다.

단계 2: USIM 정보와 사용자가 생성한 패스코드를 이용하여 모바일 ID를 생성한다. ID_U 는 모바일 ID, H 는 해쉬함수, $USIM_U$ 은 사용자 USIM 정보, pc_U 는 사용자 패스코드이다.

$$ID_U = H(USIM_U, pc_U) \in Z_{p-1}$$

단계 3: 사용자는 ID_U 를 이용하여 다음과 같이 개인키 sk_U 및 공개키 pk_U 를 생성한다. pw_U 는 사용자 패스워드로 sk_U 값이 $\mathrm{mod} P$ 에 대한 원시 근(primitive root)이 되도록 생성한다. 개인키 sk_U 는 제 3자에게 노출되지 않도록 스마트폰에는 저장하지 않고 필요할 때마다 pw_U 를 입력하여 생성한다.

$$sk_U = H(ID_U \| pw_U) \in Z_{p-1}$$

$$pk_U \equiv g^{sk_U} (\mathrm{mod} p)$$

단계 4: 사용자는 sk_U 를 이용하여 ID_U 를 서명하고 모바일 센터의 공개키 pk_{MC} 로 암호화하여 전송한다.

단계 5: 모바일 센터는 개인키 sk_{MC} 로 복호화하고 사용자 인증서의 공개키 pk_U 를 이용하여 ID_U 를 검증한다. 사용자 ID가 확인되면 모바일 센터의 개인키로 서명한 $E_{sk_{MC}}(ID_U)$를 디렉토리에 등록하고 사용자에게 전송한다.

단계 6: 사용자는 $E_{sk_{MC}}(ID_U)$를 스마트폰에 저장하고 서명 검증을 한다.

3. 부인봉쇄 디지털 서명 기법

2 장에서 생성한 (sk_U, pk_U) 를 이용하여 모바일 상거래에 적용될 수 있는 부인봉쇄 서명 기법을 제안한다. 부인봉쇄 서명은 모바일 ID로 만든 서명키를 이용하여 생성되며 검증은 서명자와 검증자 간의 도전-응답 프로토콜에 의해서 확인된다.

제안한 기법은 서명자의 동의에 의해서만 서명 검증이 가능한 부인봉쇄 성질 [4]을 만족하며 ID 기반의 모바일 PKI 시스템 [1]에 응용할 수 있다.

부인봉쇄 서명은 정의 1의 암호학적으로 안전한 유한체 GF(p) 상에서 생성되며 식 3.1과 같이 El-Gamal 서명식 [3]을 변형함으로써 서명 기법의 안전성을 이산대수 문제의 어려움(Discrete Logarithm Problem)에 근거하도록 한다.

$$k_U \cdot (HV_U + SG_U) \equiv sk_U \cdot R_U (\mathrm{mod} p-1) \quad (3.1)$$

3.1 부인봉쇄 서명 생성

단계 1: 서명자는 $p-1$ 과 서로소인 임의의 난수 k_U 를 선택하고 안전하게 보관한다. M 은 서명대상 메시지, PD 는 패딩비트, HV_U 는 M 과 PD 를 결합하여 해쉬한 결과 값이다. H 는 일방향 해쉬 함수이고 HV_U 가 원시근이 되도록 PD 값을 조정한다.

$\gcd(k_U,\ p-1) = 1$

$HV_U = H(M \| PD)$

단계 2: 난수 k_U 와 해쉬 값 HV_U 를 이용하여 다음과 같이 R_U 를 구한다.

$$R_U \equiv HV_U^{k_U} (\mathrm{mod} p)$$

단계 3: 서명자는 식 3.2를 만족하는 부인봉쇄 서명 SG_U 를 구한다. k_U 와 $p-1$은 서로소이기 때문에 SG_U 에 대한 유일한 해가 존재한다.

$$k_U \cdot SG_U \equiv sk_U \cdot R_U - k_U \cdot HV_U \ (\mathrm{mod} p-1) \quad (3.2)$$

단계 4: 서명자는 검증자에게 메시지 M , 패딩비트 PD , 부인봉쇄 서명 $(R_U,\ SG_U)$를 전송한다.

3.2 서명 검증

단계 1: 검증자는 Z_{p-1} 상에서 임의의 두 난수 $(r_1,\ r_2)$를 선택해서 서명자에게 전송할 도전 값 CH_1 을 다음과 같이 생성한다.

$$R_U^{r_1 \cdot (HV_U + SG_U)} \cdot pk_U^{R_U \cdot r_2} (\mathrm{mod} p)$$

단계 2: 검증자는 서명자에게 CH_1 을 전송한다.

단계 3: 서명자는 다음과 같이 응답 RP_1 을 생성한다.

$$RP_1 \equiv CH_1^{sk_U^{-1}} (\mathrm{mod} p)$$

$$sk_U \cdot sk_U^{-1} \equiv 1 \ (\mathrm{mod} p-1)$$

단계 4: 서명자는 검증자에게 RP_1 을 전송한다.

단계 5: 검증자는 식 3.3과 같이 RP_1 을 인증해서 서명 $(R_U,\ SG_U)$가 메시지 M 에 대한 올바른 서명인지 확인한다. 식 3.3이 성립하지 않으면 서명 $(R_U,\ SG_U)$가 메시지 M 에 대한 올바른 서명이 아니거나 서명자가 부정을 하는 경우이다.

$$RP_1 \equiv HV_U^{R_U \cdot r_1} \cdot g^{R_U \cdot r_2} \quad (\mathrm{mod} p) \quad (3.3)$$

4. 부인봉쇄 특성 분석

4.1 부인 프로토콜

부인봉쇄 서명이 올바르고 서명 검증 프로토콜이 정상적으로 수행되면 검증자의 도전 CH_1 에 대한 서명자의 응답 RP_1 은 식 3.3을 만족한다.

$$RP_1 \equiv CH_1^{sk_U^{-1}} (\mathrm{mod} p)$$

$$\equiv (HV_U^{k_U \cdot (HV_U + SG_U) \cdot r_1} \cdot g^{sk_U \cdot R_U \cdot r_2})^{sk_U^{-1}} (\mathrm{mod} p)$$

$$\equiv (HV_U^{sk_U \cdot R_U \cdot r_1} \cdot g^{sk_U \cdot R_U \cdot r_2})^{sk_U^{-1}}$$

$$(\because k_U \cdot (HV_U + SG_U) \equiv sk_U \cdot R_U (\mathrm{mod} p-1))$$

$$\equiv HV_U^{R_U \cdot r_1} \cdot g^{R_U \cdot r_2} (\mathrm{mod} p)$$

검증자는 응답 RP_1 의 인증에 실패할 경우에 서명자가 부정하는 것인지 서명이 잘못된 것인지 부인 프로토콜을 수행하여 판별한다.

단계 6: 검증자는 다음 조건을 만족하는 임의의 난수 (r_3, r_4) 를 선택해서 서명자에게 전송할 도전 CH_2 를 생성한다.

$$r_1 \cdot r_4 \neq r_2 \cdot r_3 (\mathrm{mod} p-1) \quad , (r_3, r_4) \in Z_{p-1}$$

$$CH_2 \equiv R_U^{r_3 \cdot (HV_U + SG_U)} \cdot pk_U^{R_U \cdot r_4} \quad (\mathrm{mod} p)$$

단계 7: 서명자는 검증자에게 다음과 같이 응답 RP_2 를 전송한다.

$$RP_2 \equiv CH_2^{sk_U^{-1}} (\mathrm{mod} p)$$

단계 8: 검증자는 응답 RP_1 , RP_2 를 이용해서 다음 식을 계산한다.

$$R_1 \equiv (RP_1 \cdot g^{-R_U \cdot r_2})^{r_3} (\mathrm{mod} p)$$

$$R_2 \equiv (RP_2 \cdot g^{-R_U \cdot r_4})^{r_1} (\mathrm{mod} p)$$

단계 9: R_1 과 R_2 를 비교함으로써 서명자의 부정인지 서명이 잘못된 것인지 확인한다.

$R_1 = R_2$: 서명이 잘못된 것이다.

$R_1 \neq R_2$: 서명자가 올바른 서명에 대해서 부인을 하는 경우이다.

4.2 서명 전환 프로토콜

서명자는 비밀 정보중의 일부를 공개하여 부인봉쇄 서명을 일반 서명으로 전환할 수 있다. 검증자는 서명자로부터 수신한 부인봉쇄 서명 (R_U, SG_U) 와 공개된 비밀정보를 이용하여 다음과 같이 메시지 M 에 대한 디지털 서명을 검증한다. 생성자 g 를 이용하여 식 3.1을 유도하면 다음과 같이 식 4.1을 만들 수 있다.

· 공개된 서명자의 비밀정보: g^{k_U}

· $g^{k_U \cdot (HV_U + SG_U)} \equiv g^{sk_U \cdot R_U}$

$$\equiv pk_U^{R_U} (\mathrm{mod} p) \quad (4.1)$$

식 4.1에서 k_U 가 공개되면 서명자의 개인키 sk_U 를 쉽게 구할 수 있다. 하지만 공개된 비밀정보로부터 k_U 를 구하는 문제는 다음과 같이 $GF(p)$ 상에서의 이산 대수 문제가 된다.

$r' \equiv g^{k_U} (\mathrm{mod} p)$

$k_U \equiv \log_g r' \ (\mathrm{mod} p)$

정의 1로부터 암호학적으로 안전한 유한체 $GF(p)$ 상에서의 이산 대수 문제는 계산상 불가능하다. 따라서 k_U 를 유추하는 것은 불가능하며 전환된 일반 서명의 안전성은 El-Gamal 서명 기법의 안전성과 같다 [3].

5. 모바일 콘텐츠 분배

클라이언트-서버 기반의 모바일 상거래에서 ID 기반 부인봉쇄 서명 기법을 이용하여 저작자의 권익을 보호하는 방법에 대해서 논의한다. 저작자는 모바일 콘텐츠에 부인봉쇄 서명을 하여 패키징 하고 스마트폰의 DRM 플레이어는 저작자의 서명이 검증된 콘텐츠만 재생할 수 있다고 가정한다.

(1) 콘텐츠 패키징

일반적으로 디지털 콘텐츠는 저작자 권리 보호를 위해서 저작권 정보와 함께 제어, 권한정보 등의 메타 데이터를 함께 패키징한다. 저작자는 패키징 된 콘테이너 파일에 3.1절의 서명 생성 프로토콜을 이용하여 부인봉쇄 서명을 한다. 저작자는 사용자가 올바른 콘텐츠와 라이센스를 구매 했는지 확인해 줄 수 있고, 사용자는 서명 검증을 통하여 구매한 콘텐츠 내용과 저작자에 대해서 인증할 수 있다.

(2) 구매 프로세스

단계 1: 사용자는 스마트폰을 이용하여 판매자 서버에 구매를 요청한다. 스마트폰에 저장되어 있는 모바일 ID를 판매자 서버로 전송한다.

단계 2: 판매자 서버는 모바일 센터의 공개키로 사용자 서명을 검증하고 올바른 ID이면 타임스탬프, 인증서, 모바일 ID를 함께 해쉬한다. 판매자 서버는 사용자 스마트폰으로 해쉬값을 전송한다.

단계 3: 사용자는 스마트폰에 패스코드를 입력하여 개인키를 생성하고 이를 이용하여 해쉬값에 부인봉쇄 서명을 한다. 사용자는 판매자 서버로 서명을 전송한다.

단계 4: 판매자 서버는 3.2절의 검증 프로토콜을 수행하여 올바른 사용자인지 확인하고 저작자의 서명이 첨부된 모바일 콘텐츠의 다운로드를 허용한다. 검증과정에서 판매자 서버는 난수를 발생하여 도전-응답 프로토콜을 수행하기 때문에 서명된 해쉬값을 재사용하는 재전송 공격에 대해서 안전하다.

(3) 재생 프로세스

사용자 스마트폰의 DRM 플레이어는 임의의 난수 (a, b)를 생성하여 저작자 서버로 보내고 3.2절의 검증 프로토콜을 수행한다. 서명 검증에 성공하면 사용자는 스마트폰의 플레이어로 콘텐츠를 재생할 수 있다.

콘텐츠는 저작자가 직접 판매하는 경우보다 위임을 받은 전문 판매자를 통해서 거래되는 경우가 보다 일반적이다. 일반 서명은 자체 검증 기능을 갖기 때문에 저작자는 자신이 만든 콘텐츠에 대한 구매 여부를 직접 확인할 수 없다. 판매자에 의한 부정이 가능하며 이를 방지하기 위해서는 저작자가 직접 콘텐츠 구매 여부를 확인할 수 있어야 한다.

부인봉쇄 서명은 서명자의 동의 없이는 서명 검증이 불가능하다. 제안한 서명 기법을 이용하여 서명된 콘텐츠 패키지를 온라인으로 판매할 경우에, 구매자는 서명 검증 프로토콜을 진행하여 구매한 콘텐츠에 대한 인증을 시도한다. 부인봉쇄 서명의 특성상 저작자의 동의 없이는 해당 패키지의 서명을 확인할 수 없고, 인증이 안 된 콘텐츠는 사용할 수 없도록 제어함으로써 저작자의 권익을 보장할 수 있다.

6. 결론

본 논문에서는 ID 기반의 부인봉쇄 서명 기법을 제안하였다. 스마트폰의 USIM 정보를 이용한 키 생성 프로토콜, 부인봉쇄 서명 생성 및 검증 프로토콜로 구성된다. 제안한 방법은 서명자의 동의 없이는 서명을 검증할 수 없는 부인봉쇄 성질을 만족하며 그 응용으로 모바일 상거래에서 저자자의 권익을 보호할 수 있는 방안을 제시하였다. 향후 ID 기반의 PKI 시스템을 이용한 콘텐츠 분배, 공동 저작자의 권익을 표현하는 방법, 모바일 투표 등의 응용에 적용될 수 있다.

REFERENCES

[1] Tepandi et al, “Wireless PKI Security and Mobile Voting. Computer,” IEEE Computer, Vol. 43, No. 6, pp. 54-60, 2010.

[2] Want, "iPhone: Smarter Than the Average Phone," IEEE Pervasive Computing, Vol. 9, No. 3, pp. 6-9, 2010.

[3] T.Elgamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory, Vol. IT-31, No. 4, pp. 469-472, 1985.

[4] D.Chaum, "Undeniable Signatures," Advances in Cryptology, Proceedings of CRYPTO'89, Springer-Verlag, pp. 212-216, 1990.

[5] Andre Adelsbach, Birgit Pfitzmann, Ahmad-Reza Sadeghi, "Proving Ownership of Digital Content," 3rd International Information Hiding Workshop (IHW '99), LNCS 1768, Springer-Verlag, pp. 117-133, 1999.

[6] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," Advances in Cryptology, LNCS, Springer-Verlag, pp. 47-53, 1985.

[7] Dan, Boneh, Matt and Franklin, "Identity-based encryption from the Weil pairing," Advances in Cryptology, CRYPTO 2001, Springer-Verlag, pp. 213-229, 2001.

저자소개

윤 성 현(Sung-Hyun Yun) **[종신회원]**

- 1992년 2월 : 고려대학교 컴퓨터학과 (이학학사)
- 1994년 2월 : 고려대학교 컴퓨터학과 일반대학원 (이학석사)
- 1997년 2월 : 고려대학교 컴퓨터학과 일반대학원 (이학박사)
- 1998년 3월~2002년 2월 : LG 전자 중앙연구소 선임연구원
- 2002년 3월~현재 : 백석대학교 정보통신학부 조교수

<관심분야> : 모바일 상거래 보안, DRM, 프라이버시 보호, 정보통신